UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/766,142	01/19/2001	William D. Evans	D/A0A87	1295

7590 04/27/2007

Patent Documentation Center
Xerox Corporation
Xerox Square 20th Floor
100 Clinton Ave. S.
Rochester, NY 14644

EXAMINER	
HOFFMAN, BRANDON S	
ART UNIT	PAPER NUMBER
2136	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
2 MONTHS	04/27/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/766,142
Filing Date: January 19, 2001
Appellant(s): EVANS, WILLIAM D.

Jeannette M. Walder (Reg. No. 30,698)
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed December 26, 2006, appealing from the Office action mailed June 23, 2006.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

5,787,175	Carter	7-1998
6,011,847	Follendore, III	1-2000

5,740,246 Saito 4-1998

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 103

Claims 15-29, 35, 37, 38, 41, and 42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Carter (U.S. Patent No. 5,787,175) in view of Follendore, III (U.S. Patent No. 6,011,847), and further in view of Saito (U.S. Patent No. 5,740,246).

Regarding claim 15, Carter teaches a secure content object for distributing and controlling access to a document and annotations associated with the document, comprising:

- An electronic document, the electronic document using a document encryption key, wherein access to the electronic document is available to a first set of authorized users (fig. 6, ref. num 112 and col. 13, lines 4-17);
- A first multi-key encryption table for use in a multi-key encryption method associated with the electronic document, the first table comprising at least one multi-key encryption component associated with each authorized user in the first set (fig. 6, ref. num 114-118 and col. 13, line 18 through col. 14, line 22);
- A user interface device comprising unencrypted information for identifying the electronic document and an interactive element for enabling a user to input a user authorization for access to at least a portion of the encrypted electronic

document, for inputting the user authorization to a decryption engine using the multi-key encryption method for combining the user authorization with each of the multi-key components in the first multi-key encryption key table to decrypt the encrypted header, and for combining the user authorization with each of the stored multi-key components in the second multi-key encryption key table to decrypt an annotation (fig. 9, ref. num 152 and col. 16, lines 16-29);

- Wherein upon a valid decryption of the annotation indicates the correct annotation encryption key has been found and the user is an authorized user (col. 17, lines 5-11).

Carter does not teach an encrypted header, a plurality of dummy encryption components, a plurality of annotations generated by an annotation author, wherein access to the annotations is available to the users designated by the annotation author as having access to the plurality of annotation, a second multi-key encryption table comprising at least one multi-key component associated with each authorized annotation user, and upon a valid decryption of the encrypted header, decrypting the portion of the encrypted electronic document.

Follendore, III teaches an encrypted header comprising information pertaining to the electronic document (fig. 2, ref. num 224 and col. 1, lines 22-25), a plurality of dummy encryption components, wherein the multi-key encryption table includes no information that may identify a user of the electronic document (col. 8, line 51 through

col. 9, line 7), upon a valid decryption of the encrypted header, decrypting the portion of the encrypted electronic document (fig. 2, ref. num 242).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine generating an encrypted header comprising information pertaining to the electronic document and upon valid decryption of the header, decrypting the encrypted electronic document, and generating a plurality of dummy encryption components, wherein the table includes no information identifying a user or the document, as taught by Follendore, III, with the object of Carter. It would have been obvious for such modifications because a header defines the data portion of the document. When the header is decrypted, a decryption key contained in the header for decrypting the document allows the key to be transmitted safely. Also, the dummy data provides random data to include that will make the length of the data fields the same size; this aids in the encryption process (see col. 8, line 51 through col. 9, line 7 of Follendore, III).

The combination of Carter as modified by Follendore, III still does not teach a plurality of annotations generated by an annotation author, wherein access to the plurality of annotations is available to the users designated by the annotation author as having access to the plurality of annotation and a second multi-key encryption table comprising at least one multi-key component associated with each authorized annotation user.

Saito teaches a plurality of annotations associated with the electronic document, generated by an annotation author and having been encrypted with an annotation encryption key, wherein access to the plurality of annotations is available to authorized annotation users comprising the annotation author and those users in the first set having been designated by the annotation author as having access to the plurality of annotation (col. 12, lines 20-41); and a second multi-key encryption table for use in a multi-key encryption method associated with the plurality of annotations, the second table comprising at least one multi-key component associated with each authorized annotation user (col. 12, lines 42-54).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine a multi-key table containing specific users that are allowed to access the annotations provided by the author of the annotations, as taught by Saito, with the object of Carter/Follendore, III. It would have been obvious for such modifications because user groups circumvent the problems of having to modify a document for every user, and allows a document to specify which users can access the document.

Regarding claim 16, the combination of Carter in view of Follendore, III/Saito teaches wherein the encrypted header includes an encryption marker comprising a random number sequence followed by a derivable variation of the same random number sequence, wherein a valid decryption of the encryption marker indicates that

the document encryption key has been found (see fig. 2, ref. num 230, 232, and 234 Follendore, III).

Regarding claim 17, the combination of Carter in view of Follendore, III/Saito teaches wherein the electronic document comprises content information that is formatted based on an object language having a set of formatting rules (see col. 8, lines 17-26 of Carter).

Regarding claim 18, the combination of Carter in view of Follendore, III/Saito teaches wherein the user interface device comprises a second electronic document (see col. 5, lines 34-39 of Follendore, III).

Regarding claim 19, the combination of Carter in view of Follendore, III/Saito teaches wherein the information pertaining to the electronic document comprises a user permission table for access to all or portions of the electronic document and wherein only those permitted portions of the electronic document are decrypted (see col. 8, lines 51-59 of Carter).

Regarding claim 20, the combination of Carter in view of Follendore, III/Saito teaches wherein the encrypted header and the encrypted electronic document are encrypted using different encryption keys and wherein the multi-key encryption table

includes at least one multi-key component for each encryption key (see fig. 4, ref. num 428, 430, 432, and 434 of Follendore, III).

Regarding claim 21, the combination of Carter in view of Follendore, III/Saito teaches wherein the encrypted header further comprises a fingerprint for identifying some predefined aspect of the electronic document (see fig. 2, ref. num 230, 232, and 234 of Follendore, III).

Regarding claim 22, the combination of Carter in view of Follendore, III/Saito teaches wherein the electronic document comprises a plurality of individual electronic documents and the encrypted header comprises information pertaining to each of the individual electronic documents (see col. 9, lines 44-49 of Carter).

Regarding claim 23, the combination of Carter in view of Follendore, III/Saito teaches wherein the information pertaining to the electronic document comprises a user permission table setting forth access to all or portions of each of the individual electronic documents and wherein only those permitted portions of the authorized electronic document are decrypted (see col. 8, lines 51-59 of Carter).

Regarding claim 24, the combination of Carter in view of Follendore, III/Saito teaches wherein the content information is selected from the group consisting of text,

graphics, equations, tables, spreadsheets, pictures, video files, audio files, multimedia files and binary data of unknown format (see col. 8, lines 17-26 of Carter).

Regarding claim 25, the combination of Carter in view of Follendore, III/Saito teaches wherein the object language comprises Adobe Acrobat (see col. 8, lines 17-26 of Carter).

Regarding claim 26, the combination of Carter in view of Follendore, III/Saito teaches wherein the object language comprises a language which interprets Microsoft Word documents (see col. 8, lines 17-26 of Carter).

Regarding claim 27, the combination of Carter in view of Follendore, III/Saito teaches wherein the encrypted header includes an encryption marker comprising a random number sequence followed by a derivable variation of the same random number sequence, wherein a valid decryption of the encryption marker indicates the header encryption key has been found (see fig. 2, ref. num 230, 232, and 234 Follendore, III); and wherein the encrypted electronic document includes an encryption marker comprising a random number sequence followed by a derivable variation of the same random number sequence, wherein a valid decryption of the encryption marker indicates the document encryption key has been found (see fig. 2, ref. num 234, 236, and 238 of Follendore, III).

Regarding claim 28, the combination of Carter in view of Follendore, III/Saito teaches wherein the electronic document includes a document ID and wherein the document encryption key includes a combination of the document ID, the user information and the multi-key components, for each authorized user (see fig. 4, ref. num 92 and 96 and col. 13, line 63 through col. 14, line 5 of Carter).

Regarding claim 29, the combination of Carter in view of Follendore, III/Saito teaches wherein the electronic document comprises a first electronic document and an annotation associated therewith, wherein the annotation is encrypted using an encryption key associated with a user generating the annotation (see fig. 10, ref. num 176, 180 and 182 and col. 20, lines 51-65 of Carter); and wherein the encrypted header includes information pertaining to the first electronic document and the annotation (see col. 9, lines 56-61 of Follendore, III).

Regarding claim 35, Carter teaches a method for creating a secure content object for distributing and controlling access to a document and annotations associated with the document, comprising:

- Providing an electronic document, wherein access to the electronic document is available to a first set of users (fig. 4, ref. num 54,90);
- Responsive to a first user from the first set of users, generating a plurality of annotations pertaining to the electronic document using the document language (fig. 10, ref. num 176);

- Encrypting each annotation using an annotation encryption key associated with the first user generating the particular annotation, wherein access to an encrypted annotation is available to authorized users having access to the respective annotation encryption key (fig. 10, ref. num 180 and 182 and col. 20, lines 51-65);

For each annotation encryption key:

- Generating a multi-key encryption table for use in a multi-key encryption method, the table comprising at least one multi-key component (fig. 6, ref. num 114, 116, and 118 and col. 13, line 18 through col. 14, line 22);
- Providing a user interface for enabling a user to input a user authorization for access to at least a portion of an encrypted annotation (fig. 9, ref. num 152 and col. 16, lines 16-29);
- Wherein, responsive to an input user authorization, combining the input user authorization with each of the stored multi-key components in the multi-key encryption key table to decrypt the annotation, wherein valid decryption of the annotation indicates the correct annotation encryption key has been found (fig. 11, ref. num 192); and
- Access to the encrypted electronic document is available to the first set of users and access to the encrypted annotations in the separate file is provided only to authorized users (fig. 11, ref. num 192).

Carter does not teach associating the plurality of annotations with the first user, designating which users in the first set of users are authorized users have access to the plurality of annotations, associating with each authorized user having been designated by the first user as having access to the annotation, concatenating the plurality of encrypted annotations in a second electronic document, and merging the second electronic document and the encrypted electronic document into a third electronic document.

Follendore, III teaches concatenating the plurality of encrypted annotations in a second electronic document (fig. 2, ref. num 224), and merging the second electronic document and the encrypted electronic document into a third electronic document (fig. 2, ref. num 222 and 224 contained within 218).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine concatenating the annotations in a second document and merging the second electronic document and the encrypted electronic document into a third electronic document, as taught by Follendore, III, with the method of Carter. It would have been obvious for such modifications because the annotations can become many for only one file. By combining the annotations into their own electronic document, they can be handled on their own with their own keys separate from the electronic document.

The combination of Carter as modified by Follendore, III still does not teach associating the plurality of annotations with the first user, designating which users in the first set of users are authorized users have access to the plurality of annotations, associated with each authorized user having been designated by the first user as having access to the annotation.

Saito teaches associating the plurality of annotations with the first user, designating which users in the first set of users are authorized users have access to the plurality of annotations, associated with each authorized user having been designated by the first user as having access to the annotation (col. 12, lines 20-54).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine associating the authorized users for viewing the annotations in the table, as prescribed by the annotation author, as taught by Saito, with the object of Carter/Follendore, III. It would have been obvious for such modifications because user groups circumvent the problems of having to modify a document for every user, and allows a document to specify which users can access the document.

Regarding claim 37, the combination of Carter in view of Follendore, III/Saito teaches further comprising the step of:

- Encrypting the first electronic document using a document encryption key, wherein access to the encrypted electronic document is provided only to the first set of users (see fig. 6, ref. num 112 and col. 13, lines 4-17 of Carter);
- Generating a multi-key encryption table for us in a multi-key encryption method, the table comprising at least one multi-key component associated with each of the first set of users (see fig. 6, ref. num 114, 116, and 118 and col. 13, line 18 through col. 14, line 22 of Carter);
- Generating an encrypted header comprising information pertaining to the electronic document (see fig. 2, ref. num 224 of Follendore, III);
- Providing a user interface for enabling a user to input a user authorization for access to at least a portion of the encrypted document (see fig. 9, ref. num 152 and col. 16, lines 16-29 of Carter);
- Combining the user authorization with each of the stored multi-key components in the multi-key encryption key table to decrypt the encrypted header, wherein valid decryption of the encryption header indicates the document encryption key has been found (see fig. 9, ref. num 160 and 162 and col. 16, line 60 through col. 17, line 26 of Carter, and see fig. 2, ref. num 242 of Follendore, III).

Regarding claim 38, the combination of Carter in view of Follendore, III/Saito teaches further comprising adding an unencrypted header identifying the generating user to each encrypted annotation (see fig. 2, ref. num 220 of Follendore, III).

Regarding claim 41, the combination of Carter in view of Follendore, III/Saito teaches wherein the encrypted header includes an encryption marker comprising a random number sequence followed by a derivable variation of the same random number sequence, wherein a valid decryption of the encryption marker indicates the annotation encryption key has been found (see fig. 2, ref. num 230, 232, and 234 Follendore, III).

Regarding claim 42, the combination of Carter in view of Follendore, III/Saito teaches wherein the separate file and the electronic document are stored in different locations (see col. 9, lines 37-43 of Follendore, III).

(10) Response to Argument

Applicant argues:

a. Carter does not teach access to the plurality of annotations is available to authorized annotation users comprising the annotation author and those users in the first set having been designated by the annotation author as having access to the plurality of annotations (page 8, section A1).

b. Follendore, III does not teach access to the plurality of annotations is available to authorized annotation users comprising the annotation author and those users in the first set having been designated by the annotation author as having access to the plurality of annotations (page 9, section A2).

c. Saito does not teach access to the plurality of annotations is available to authorized annotation users comprising the annotation author and those users in the first set having been designated by the annotation author as having access to the plurality of annotations (page 9, section A3).

d. Saito does not provide any means for ensuring that the second user is an authorized user; any recipient of the data that has been encrypted by the first user can receive a decryption key from Saito's copyright management system (page 10, section A4).

Regarding argument (a), examiner disagrees with applicant. Carter teaches users of a workgroup can view annotations made to a document and any user who is not a member of the workgroup cannot view the annotations. Applicant argues that Carter does not teach encrypting annotations to a document separately from the document (see page 8, last paragraph of applicant's appeal brief). However, Saito (as argued below with argument (c)) shows this by using a different key to encrypt the annotations. The member's of the workgroup of Carter are one set of members who have access to annotations made by other member's of the workgroup (see figure 9, reference numbers 160 and 162). Users who are not in the workgroup do not have access to the annotations made by a member of the workgroup (see figure 9, reference number 156 of Carter).

Regarding argument (b), examiner disagrees with applicant. Follendore, III was cited for teaching an encrypted header comprising information pertaining to the

electronic document, a plurality of dummy encryption components, wherein the multi-key encryption table includes no information that may identify a user of the electronic document, and upon a valid decryption of the encrypted header, decrypting the portion of the encrypted electronic document (see figure 2, reference number 224 and 242, column 1, lines 22-25 and column 8, line 51 through column 9, line 7 of Follendore, III). These limitations discuss attaching labels to a header of a document. Follendore, III does not teach the limitations pertaining to controlling access to certain annotations based on user authorization, as acknowledged by the examiner in the rejection above.

Regarding argument (c), examiner disagrees with applicant. Saito teaches that an original document is edited by an editor (annotation author) and the edited material is encrypted with a key. Users are able to decrypt the edited material, along with the original document. Applicant contends that the users in Saito are able to decrypt the entire edited section, as opposed to a portion of edited data, as claimed. However, the claim states that ***at least a portion*** of the encrypted electronic document is accessed by the authorized users. When interpreting the language of a portion, three scenarios come into play: the entire document means the whole document, a portion of the document means a subset, or part, of the whole document, and at least a portion of the document means at least a subset, or part, of the whole document, but also means up to and including the whole document. Therefore, Saito, which teaches accessing the whole encrypted document, also teaches accessing ***at least a portion*** of the encrypted document. Additionally, Saito teaches encrypting annotations to a document separately from the document (see column 12, lines 20-54 of Saito) because of the use of a

different crypt key to encrypt an edited document (as admitted by applicant at page 9, section A3).

Regarding argument (d), examiner disagrees with applicant. Saito, by himself, does not teach restricting access to certain users, but restricts access to anyone who possesses the encrypted document with the signature of the author contained therein (see column 12, lines 48-54 of Saito). However, the combination of Carter and Saito teaches restricting access to the annotations to certain users of the system. Carter teaches, in figure 2, reference number 44, figure 9, reference number 152, and column 16, lines 16-29, that the collaborative access controller restricts access to certain users based on user id and password entry. Only the users that are designated as being able to decrypt the document are allowed by entering the user id and password given to them.

Carter, Follendore III, and Saito are analogous and combinable references because each reference discusses document control (preventing and allowing certain users to gain access to parts or all of a document).

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Brandon Hoffman

Conferees:

Taghi Arani

Kim Vu